

CLAIMS

What is claimed is:

1. A method comprising:
establishing a protected communications channel with a computing system, the computing system providing SIM AAA capabilities without the use of a discrete hardware SIM device; and
provisioning SIM secret data to the computing system over the protected communications channel.
2. The method of claim 1 wherein provisioning SIM secret data includes provisioning at least one of identity secrets, key secrets, information to initialize data objects, information to initialize operator-specific cryptography algorithms, and information to install or update applications, parameters, tools or utilities.
3. The method of claim 1 wherein establishing a protected communications channel includes using a protected key exchange mechanism.
4. The method of claim 3 wherein provisioning SIM secret data includes encrypting the SIM secret data.

5. A method comprising:
using SIM capabilities provided by a computing system without a discrete hardware SIM device for user authorization, authentication and accounting in association with a subscription account; and
providing a subscription account for access by the computing system.
6. The method of claim 5 wherein providing the subscription account includes providing a wireless network access account.
7. The method of claim 6 wherein using SIM capabilities provided by a computing system includes using SIM capabilities provided by a laptop computing system.
8. The method of claim 5 wherein providing the subscription account includes providing a wired network access account.
9. The method of claim 5 wherein using SIM capabilities includes using a protected execution environment provided by a laptop computing system.
10. The method of claim 5 wherein providing the subscription account includes providing location-based services.

11. A computer-accessible medium storing information, that when accessed by a computing system causes the computing system to:

- establish a protected communications channel with a computing system, the computing system to provide SIM AAA capabilities without the use of a discrete hardware SIM device; and
- provision SIM secret data to the computing system over the protected communications channel.

12. The computer-accessible medium of claim 11 wherein provisioning SIM secret data includes provisioning at least one of identity secrets, key secrets, information to initialize data objects, information to initialize operator-specific cryptography algorithms, and information to install or update applications, parameters, tools or utilities.

13. The computer-accessible storage medium of claim 12 wherein provisioning includes encrypting the secret data prior to providing the secret data to the computing system.

14. The computer-accessible storage medium of claim 11 wherein establishing a protected communications channel includes participating in a bilateral key exchange.

15. The computer-accessible storage medium of claim 14 wherein establishing a protected communications channel includes receiving authentication information from the computing system.

16. A method comprising:
authenticating and authorizing a user of a subscription account at least in part by using Subscriber Identity Module (SIM) compliant authentication and authorization capabilities on a computing system that provides the SIM-compliant authentication and authorization capabilities without the use of a discrete SIM hardware device; and
providing user access to the subscription account upon receipt of predetermined credentials.

17. The method of claim 16 wherein providing user access to the subscription account includes providing user access to a wireless network account.

18. The method of claim 17 wherein providing user access to wireless network account includes providing access to one of a GSM/GPRS network, a 3G network and a Personal Handyphone Network.

19. The method of 16 wherein providing user access to the subscription account includes providing user access to a location-based services account.

20. An apparatus comprising:
a server having access to a network; and
a provisioning module stored on the server, the provisioning module, when executed by the provisioning server, to participate in provisioning Subscriber Identity Module (SIM) secret data to a computing system, the computing system to provide SIM-compliant authentication, authorization and accounting capabilities without the use of a discrete hardware SIM device.

21. The apparatus of claim 20 wherein the network is one of a GSM/GPRS, 3G, Personal Handyphone System (PHS) and a CDMA network.

22. The apparatus of claim 20 wherein the network is a wireless network.

23. The apparatus of claim 20 wherein the network is a wired network.

24. The apparatus of claim 20 wherein the provisioning module, when executed by the server, further operates to encrypt the SIM secret data to be provided to the computing system.

25. The apparatus of claim 24 wherein the provisioning module, when executed by the server, further operates to participate in a bilateral key exchange with the computing system over the network.

26. The apparatus of claim 20 wherein the computing system is further to store the SIM secret data in an encrypted format on a mass storage device of the computing system.

27. The apparatus of claim 26 wherein the computing system is further to store an encrypted bulk encryption key to be used to decrypt the encrypted SIM secret data.

28. The apparatus of claim 27 wherein the computing system further includes a hardware token to provide a second key to encrypt the bulk encryption key.

29. The apparatus of claim 20 wherein the server is further to control access by the computing system to a service, the server to provide access to the service by the computing system upon authorization and authentication of the computing system using the SIM-compliant authentication, authorization and accounting capabilities.